SESSION DE 2005

concours externe
de recrutement de professeurs agrégés

section : mathématiques

composition de mathématiques générales

durée : 6 heures

Les calculatrices électroniques de poche sont autorisées, conformément à la circulaire 99-186 du 16 novembre 1999.

La qualité de la rédaction et de la présentation, la clarté et la précision des raisonnements constitueront un élément important pour l'appréciation des copies.

Les corps considérés dans le problème sont supposés commutatifs. Pour tout entier $n \geqslant 1$, on note $M_n(\mathbb{C})$ l'anneau des matrices carrées à n lignes et n colonnes à coefficients dans $\mathbb{C}$, $M_n(\mathbb{Z})$ le sous-anneau de $M_n(\mathbb{C})$ formé des matrices à coefficients dans $\mathbb{Z}$, et $C_n(\mathbb{Z})$ l'ensemble des vecteurs colonnes à n lignes à coefficients dans $\mathbb{Z}$.

Pour tout ensemble Z, on note $S(Z)$ le groupe des bijections de Z sur lui-même. Si X et Y sont deux ensembles, on note Y^X l'ensemble des applications de X dans Y.

I.

1) Soit A une matrice de $M_n(\mathbb{C})$.

1-a) Montrer que $A \in M_n(\mathbb{Z})$ si et seulement si, pour tout X dans $C_n(\mathbb{Z})$, on a $AX \in C_n(\mathbb{Z})$.

1-b) Soit A une matrice de $M_n(\mathbb{Z})$ dont le déterminant, noté $\det A$, est non nul et soit A^{-1} son inverse dans $M_n(\mathbb{C})$. Montrer que $A^{-1} \in M_n(\mathbb{Z})$ si et seulement si $|\det A| = 1$.

2) On munit $\mathbb{R}^n$ d'un produit scalaire noté $<,>$. Pour toute partie Y de $\mathbb{R}^n$, on note

$$Y^* = \{x \in \mathbb{R}^n \mid \forall y \in Y,\ < x, y > \in \mathbb{Z}\}.$$

Si $B = (v_i)_{1 \leqslant i \leqslant n}$ est une base de $\mathbb{R}^n$, on note

$$L_B = \left\{ \sum_{i=1}^{n} m_i v_i \;\middle|\; (m_1, \ldots, m_n) \in \mathbb{Z}^n \right\}$$

le sous-groupe additif de $(\mathbb{R}^n, +)$ engendré par B ; de plus, on note G_B la matrice de $<,>$ dans la base B, c'est-à-dire la matrice symétrique définie positive dont le (i, j)-ième coefficient vaut $< v_i, v_j >$.

2-a) Soit $x \in \mathbb{R}^n$. Montrer que $x \in L_B^*$ si et seulement s'il existe $X \in C_n(\mathbb{Z})$ tel que $G_B^{-1}X$ est le vecteur colonne formé des composantes de x dans la base B.

2-b) On suppose que $L_B \subset L_B^*$. Montrer que $G_B \in M_n(\mathbb{Z})$, et que $\det G_B = 1$ si et seulement si $L_B^* = L_B$.

3) On note $(e_i)_{1 \leqslant i \leqslant n}$ la base canonique de $\mathbb{R}^n$ et $(e_i^*)_{1 \leqslant i \leqslant n}$ sa base duale. Soit L un sous-groupe du groupe additif $(\mathbb{R}^n, +)$, tel que $2\mathbb{Z}^n \subset L \subset \mathbb{Z}^n$. Pour $1 \leqslant i \leqslant n$, on pose $L_i = L \cap F_i$, où F_i est le sous-espace vectoriel de $\mathbb{R}^n$ engendré par $\{e_i, \ldots, e_n\}$.

3-a) Montrer que, pour tout i, $1 \leqslant i \leqslant n$, il existe $a_i \in \{1, 2\}$, tel que $e_i^*(L_i) = a_i\mathbb{Z}$.

3-b) Pour $1 \leqslant i \leqslant n$, soit $u_i \in L_i$ tel que $e_i^*(u_i) = a_i$. Montrer que $(u_i)_{1 \leqslant i \leqslant n}$ engendre L et est une base de $\mathbb{R}^n$.

4) Soit C un $\mathbb{Z}/2\mathbb{Z}$-sous-espace vectoriel de $(\mathbb{Z}/2\mathbb{Z})^n$, et $L = \rho^{-1}(C)$, où ρ est l'application de $\mathbb{Z}^n$ sur $(\mathbb{Z}/2\mathbb{Z})^n$ définie par $\rho(m_1, \ldots, m_n) = (\tilde{m}_1, \ldots, \tilde{m}_n)$, $\tilde{m}$ étant la classe de m modulo 2.

Dans cette question, le produit scalaire $<,>$ est défini par $< x, y > = \dfrac{1}{2} \sum_{i=1}^{n} x_i y_i$, pour tout couple de vecteurs $x = (x_1 \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ de $\mathbb{R}^n$. De plus, on munit $(\mathbb{Z}/2\mathbb{Z})^n$ de la forme bilinéaire non dégénérée, définie, pour tout couple de vecteurs $x = (x_1 \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ de $(\mathbb{Z}/2\mathbb{Z})^n$, par $x.y = \sum_{i=1}^{n} x_i y_i$.

4-a) Montrer qu'il existe une base B de $\mathbb{R}^n$ engendrant L, et que $L^* = \rho^{-1}(C^\perp)$, où $C^\perp$ est l'orthogonal de C relativement à la forme bilinéaire définie ci-dessus.

4-b) On suppose que $C \subset C^\perp$. Montrer que G_B est à coefficients entiers, et que $\det G_B = 1$ si et seulement si $C = C^\perp$.

II.

1) Soit K un corps, A un K-espace affine de dimension finie $r \geqslant 3$, et F le sous-espace vectoriel de K^A formé des fonctions affines $f:\ A \to K$.

1-a) Montrer que F est de dimension $r+1$.

1-b) Soit $G_{aff}(A)$ le groupe affine de A, c'est-à-dire le groupe des applications affines bijectives de A dans lui-même. Montrer que $G_{aff}(A) = \{\sigma \in S(A) \mid \forall f \in F,\ f \circ \sigma \in F\}$.

2) On suppose ici que K est un corps fini et on note q son nombre d'éléments. Soit $\cdot$ la forme bilinéaire non dégénérée sur K^A définie, pour $f, g \in K^A$, par $f \cdot g = \sum_{x \in A} f(x)g(x)$. On note $F^\perp$ l'orthogonal de F relativement à cette forme bilinéaire.

2-a) Soit $f \in F$, non constante. Montrer que, pour tout $a \in K$, l'ensemble $f^{-1}(\{a\})$ a q^{r-1} éléments.

2-b) Montrer que $F \subset F^\perp$, et que $F = F^\perp$ si et seulement si $q = 2$ et $r = 3$.

3) Dans cette question, on suppose que $K = \mathbb{Z}/2\mathbb{Z}$ et que A est l'espace affine K^3, dont on numérote les points par $P_0 = (0,0,0)$, $P_1 = (1,0,0)$, $P_2 = (1,1,0)$, $P_3 = (0,1,1)$, $P_4 = (1,0,1)$, $P_5 = (0,1,0)$, $P_6 = (0,0,1)$ et $P_7 = (1,1,1)$.

Soit $\varphi:\ K^A \to K^8$ l'application linéaire bijective définie par $f \mapsto (f(P_0), f(P_1), \ldots, f(P_7))$ et H le sous-espace vectoriel de K^8 égal à $\varphi(F)$.

3-a) Combien H possède-t-il d'éléments ayant exactement 4 composantes non nulles ?

3-b) Montrer qu'une base de H est

$$\{(1,1,1,1,1,1,1,1), (0,1,1,0,1,0,0,1), (0,0,1,1,0,1,0,1), (0,0,0,1,1,0,1,1)\}.$$

4) On utilise dans cette question les notations de la question I-4. On suppose que $n = 8$ et $C = H$.

4-a) Montrer que : $\inf\{< x, x > \mid\ x \in L - \{0\}\} = 2$.

4-b) Combien L possède-t-il d'éléments x tels que $< x, x >= 2$?

4-c) Déduire de ce qui précède

i) L'existence d'une matrice symétrique définie positive dans $M_8(\mathbb{Z})$, de déterminant 1 et dont les termes diagonaux sont pairs.

ii) L'existence d'une base B de l'espace euclidien usuel $\mathbb{R}^8$, possédant la propriété suivante : soit S l'ensemble des boules fermées de rayon 1 (pour la norme euclidienne) centrées en les points de L_B. Les éléments de S sont deux à deux d'intérieurs disjoints, et chaque élément de S est tangent[1] à 240 autres.

[1] deux boules fermées sont dites tangentes si la distance de leurs centres est égale à la somme de leurs rayons.

Dans la suite du problème, k désigne un corps de caractéristique différente de 2, $Q = \{x \in k \mid \exists y \in k - \{0\}, x = y^2\}$ l'ensemble de ses carrés non nuls, et $X = \mathbb{P}^1(k) = k \cup \{\infty\}$ la droite projective sur k. On rappelle que l'application $\alpha :\ \mathrm{GL}_2(k) \to S(X)$ qui à $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ associe l'homographie $\alpha(M) :\ x \mapsto \dfrac{ax+b}{cx+d}$ est un morphisme de groupes. On note $\mathrm{Ker}(\alpha)$ son noyau, c'est-à-dire $\alpha^{-1}(\{\mathrm{id_X}\})$.
On rappelle également que, si $c = 0$, on a $\alpha(M)(\infty) = \infty$, et que, si $c \neq 0$, $\alpha(M)(\infty) = \dfrac{a}{c}$ et $\alpha(M)\Big(-\dfrac{d}{c}\Big) = \infty$.
On note $\mathrm{SL}_2(k)$ le sous-groupe de $\mathrm{GL}_2(k)$ formé des matrices de déterminant 1 et $N = \mathrm{PSL}_2(k)$ l'image de $\mathrm{SL}_2(k)$ par α.

III.

1-a) Montrer que $\mathrm{SL}_2(k) \cap \mathrm{Ker}(\alpha) = \{-I_2,\, I_2\}$, où $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

1-b) Soit $M \in \mathrm{GL}_2(k)$; montrer que $\alpha(M) \in N$ si et seulement si $\det(M) \in Q$.

2) Si k est un corps fini à q éléments, calculer le nombre d'éléments de N en fonction de q.

3) Montrer que les homographies $x \mapsto h_i(x) = ix$ (pour $i \in Q$), $x \mapsto t_j(x) = x + j$ (pour $j \in k$) et $x \mapsto w(x) = -\dfrac{1}{x}$ appartiennent à N et l'engendrent.

4) Soit f un élément d'ordre 2 de N.

4-a) Montrer que f est conjugué dans N à une homographie de la forme $x \mapsto w_i(x) = -\dfrac{i}{x}$, avec $i \in Q$.

4-b) Montrer que si k a au moins cinq éléments, il existe un conjugué g de f dans N ne commutant pas avec f (on pourra calculer $t_a \circ w_i \circ t_a^{-1}$).

5) Soit A un $\mathbb{Z}/2\mathbb{Z}$-espace affine de direction $\overrightarrow{A}$ et $G_{aff}(A)$ son groupe affine.

5-a) Montrer que, si P est un sous-groupe de $G_{aff}(A)$ ne contenant pas de translation différente de l'application identique, alors P est isomorphe à un sous-groupe de $\mathrm{GL}(\overrightarrow{A})$.

5-b) On suppose que k a au moins cinq éléments. Montrer que, si N est isomorphe à un sous-groupe de $G_{aff}(A)$, il est isomorphe à un sous-groupe de $\mathrm{GL}(\overrightarrow{A})$.

IV.

On note $\mathbf{1} :\ X \to \mathbb{Z}/2\mathbb{Z}$ la fonction constante égale à 1, $\mathbf{0} :\ X \to \mathbb{Z}/2\mathbb{Z}$ la fonction nulle, on note $-Q = \{-x \mid x \in Q\}$ et on suppose que k vérifie la propriété $(*)$ suivante :

$(*)$ $\quad$ *$k - \{0\}$ est l'union disjointe de Q et $-Q$.*

1) Montrer que, si k a q éléments, l'hypothèse $(*)$ est équivalente à $q \equiv -1 \mod 4$.

On note $u : X \to \mathbb{Z}/2\mathbb{Z}$ l'application qui vaut 1 si $x \in Q \cup \{\infty\}$ et 0 sinon. Pour tout élément $r \in k$, on pose $u_r = u \circ t_r$.

2-a) Montrer que, pour tout $i \in Q$ et $r \in k$, on a $u_r \circ h_i = u_{r/i}$.

2-b) Montrer que $u + u \circ w = \mathbf{1}$, puis que $u + u_{w(r)} + u_r \circ w = \begin{cases} \mathbf{1} & \text{si } r \in Q \\ \mathbf{0} & \text{si } r \in -Q \end{cases}$.

2-c) On suppose que k est un corps fini. Montrer que $\sum_{r \in k} u_r = \mathbf{1}$.

Soit R le sous-espace vectoriel de $(\mathbb{Z}/2\mathbb{Z})^X$ engendré par les fonctions u_r, $r \in k$. Montrer que

$$\mathrm{PSL}_2(k) \subset \{\sigma \in S(X) \mid \forall f \in R,\ f \circ \sigma \in R\}.$$

3) On suppose ici que $k = \mathbb{Z}/7\mathbb{Z}$. Soit $\psi : (\mathbb{Z}/2\mathbb{Z})^X \to (\mathbb{Z}/2\mathbb{Z})^8$ l'application linéaire bijective définie par

$$f \mapsto \Big(f(\overline{0}), f(\overline{1}), f(\overline{2}), f(\overline{3}), f(\overline{4}), f(\overline{5}), f(\overline{6}), f(\infty)\Big),$$

où, pour tout entier $x \in \mathbb{Z}$, $\overline{x}$ est la classe de x modulo 7.

3-a) Montrer que $\psi(R) = H$, où H est le sous-espace vectoriel de $(\mathbb{Z}/2\mathbb{Z})^8$ défini en II.3.

3-b) En déduire que $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$ est isomorphe à $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$.